

# IRS News Release

---

Media Relations Office

Washington, D.C.

Media Contact: 202.622.4000

[www.irs.gov/newsroom](http://www.irs.gov/newsroom)

Public Contact: 800.829.1040

---

## **The Official Internal Revenue Service Web Site Is IRS.gov**

FS-2009-4, January 2009

WASHINGTON — Millions of taxpayers this filing season will go online to retrieve tax forms, publications and other information from the Internal Revenue Service. Unfortunately, some of those people will end up at Web sites that have no affiliation with the IRS.

The official Web site for the Internal Revenue Service is [IRS.gov](http://www.irs.gov), and all [IRS.gov](http://www.irs.gov) Web page addresses begin with <http://www.irs.gov/>.

There are many phony Internet sites that impersonate federal or state tax agency sites. Scammers operate these sites as a means of getting visitors to reveal personal and financial information that can be used to steal the visitors' identity and access their bank accounts, credit cards and more.

In addition to Web sites established by scammers, there are commercial Internet sites that often resemble the authentic IRS site or contain some form of the IRS name in the address but end with a .com, .net, .org or other designation instead of .gov. These sites have no connection to the IRS.

### **Bogus E-Mail, Fraudulent Web Sites: Identity Theft Tools**

It is important to be vigilant when conducting any transactions online. Victims of identity theft can spend years — and a lot of their own money — cleaning up the mess thieves have made of their names and credit records. Victims may lose job opportunities, may be refused loans for education, housing or cars, or even face arrest for crimes they did not commit.

Identity theft can happen in a number of ways.

For example, it can start with an Internet search for the IRS or tax-related information that results in links to Web sites run by scam artists.

Taxpayers may also receive e-mail that claims to come from the IRS. Such messages often direct the recipient to phony Web sites that ask for personal and financial information that can be used to steal the recipient's identity. Bogus e-mail such as this has been received by individuals, businesses and even tax-exempt organizations.

As a rule, the IRS does not send unsolicited e-mail and does not use e-mail to discuss tax account information with — or request personal or financial information from — taxpayers. Additionally, the IRS never asks people for PIN numbers or passwords for their credit card, bank or other financial accounts.

The recipient of this type of e-mail should never open an attachment within the e-mail or click on any link within the e-mail. When clicked, the attachments or links in the bogus e-mails may send the recipient to phony Web sites or download malicious computer code onto the recipient's computer. Malicious code may look for passwords and other information and send them to the scammer, allowing the scammer to control the victim's computer, or more.

The safest way to access a federal or state tax agency Web site is to close the e-mail and type the address of the site directly in the Internet browser.

Phony Web sites often look legitimate because much of their content is directly copied from an actual page on the IRS Web site, which is then modified by the fraudsters for their own purposes. The bogus site might look like the IRS.gov home page or may appear to be one of the pages within IRS.gov Web site. In fact, a common phishing scam that has often circulated after the April 15 filing deadline, when many taxpayers are still awaiting their tax refunds, uses refunds as its lure. The scam usually sends recipients who click on the link contained in the e-mail to a phony IRS "[Where's My Refund?](#)" Web site that is modified to elicit personal and financial information that the scammers can steal.

The contents vary but they often claim the recipient is entitled to a tax refund, will be paid for participating in an online survey or is under investigation or audit. Some e-mails have solicited for charitable donations. More information on the scam e-mails is available in articles and news releases on the IRS.gov.

Those who have received a questionable e-mail claiming to come from the IRS may forward it to a mailbox the IRS has established to receive such e-mails, [phishing@irs.gov](mailto:phishing@irs.gov). An article on IRS.gov titled "[How to Report and Identify Phishing, E-mail Scams and Bogus IRS Web Sites](#)" contains instructions. Following the instructions will help the IRS track suspicious e-mail to its origins and shut down potential scams.

## **How to Find State Tax Agency Web Sites**

Taxpayers may also find links on IRS.gov to official state tax agency Web sites. These may be found by entering the words "state links" in the search box in the upper right-hand corner of any page. Links to all of the states and the District of Columbia are available on the page that opens. Taxpayers may also visit the Web site of the Federation of Tax Administrators at <http://www.taxadmin.org/> for their state tax needs. The FTA is an association of the tax agencies in the 50 states, District of Columbia, New York City and Puerto Rico.